METHODS AND SYSTEMS FOR DETERMINING THE RELIABILITY OF TRANSACTIONS

BACKGROUND OF THE INVENTION

Many sellers offer products or services without requiring the physical presence of the buyer. Buyers usually contact such sellers by phone, fax, Short Message Service (SMS), email, or through the seller's website.

In order to pay the seller, the remote buyer will often provide an identifier of a chargeable account, such as a credit card number, debit card number, checking account number, bank account identifier or phone number. The seller then uses this identifier to charge the account.

Fraudsters who gain access to an account identifier could contact a seller, provide the identifier to the seller, and cause the true owner of the account to be charged.

In order to prevent such fraudulent transactions, sellers deploy various methods to verify that an account belongs to the buyer. One such method is requiring the buyer to provide personal details of the account owner, which are then compared with information associated with the account at a trustable third party, such as the organization administering the account (the 'account issuer') or a transaction processing service, which receives account information from multiple sellers.

For example, sellers often require buyers to provide a mailing address of a credit card account owner (usually the address where the owner receives his credit card bills, known as the billing address), and compare this mailing address to addresses stored on the databases of the bank that issued the card. The seller may of course do the same with any other personal details of the account owner, such as a name, a phone number, a government-issued identifier (e.g. driver's license number), an email address etc.

Sellers use a variety of methods to contact the issuer when performing such a comparison, such as speaking with a representative of the account issuer over the phone, exchanging faxes with the issuer, or using the issuer's IVR (Interactive Voice Response) system.

Additionally, banks in the United States, Canada and the United Kingdom offer an automatic service for verifying billing addresses called AVS (Address Verification System). To use AVS, the seller sends to the bank, over the credit card data network, an AVS request containing the numeric portion of the billing address (house number + zip code) and the card number, and receives a response that describes which of the elements in the AVS request match the bank's records. Furthermore, some banks allow cardholders to add an alternate address to the account, so the cardholders could provide sellers with this address without causing AVS to fail. United States published patent application 2003/0023541, the entirety of which is herein incorporated by reference, discloses methods and systems for verifying billing addresses and alternate billing addresses.

By requiring buyers to present personal details at the time of transaction, and by comparing these presented personal details with previously obtained and stored personal details, sellers expect to decrease the incidence of fraud, as fraudsters are less likely to know specific personal details than the legitimate account owner. In practice, fraudsters have found simple ways to gain access to these personal details and thus this method is now considered ineffective.

Sellers may complicate fraud attempts by performing some action based on the personal details, such as shipping goods only to the verified billing address, calling the verified phone number to check that the account owner is aware of the transaction, or sending an email to the verified email account. The first two methods (shipping to the billing address and calling the account owner) are currently used by many sellers, whereas the last method (sending an email) is not, since banks do not usually have account owners' email addresses and do not usually provide means for verifying them. US Patents 5757917 and 5826241 the entirety of which is herein incorporated by reference, and PCT Applications WO03/017049 and WO01/69549 the entirety of which is herein incorporated by reference describe methods for verifying payments by email, in which buyers need to register their account identifiers and email addresses in advance.

Nevertheless, fraudsters could still circumvent such measures by contacting the issuer, impersonating the legitimate account owner and requesting that the issuer update stored personal details. For example, credit card issuers in the United States often verify callers by requiring the Social Security Number (SSN) of the cardholder. A

fraudster who gains access to the SSN can thus change the billing address (or add an alternate address) to an address where he can receive merchandise, or change the phone number to a number where he can receive calls. In another example, a fraudster may use stolen information of another person to open a new credit card account, and provide any additional personal details he wants.

There is an ongoing need for techniques for assessing the reliability of transactions submitted by buyers. Furthermore, there is a recognized need for methods and systems for verifying and assessing the reliability of personal details presented in transactions of remote buyers, particularly in the context of e-commerce.

BRIEF SUMMARY OF THE INVENTION

In accordance with some aspects of the present invention, a method is provided for determining the reliability of a transaction involving an account identifier identifying a chargeable account. Specifically, methods disclosed in accordance with some embodiments include receiving the account identifier; and providing at least one reliability indicator indicating the estimated likelihood that at least one stored personal detail associated with the chargeable account was submitted fraudulently.

In exemplary embodiments, the methods of the present invention provide tools for helping sellers and other interested parties to distinguish between a buyer who is the true and legitimate owner of a chargeable account, and a buyer who is attempting to impersonate the true account owner and to defraud the seller or other interested parties.

Not wishing to be bound by theory, it is now disclosed that fraudsters are known to contact account issuers, impersonate the legitimate account owner, request that the issuer update stored personal details, and execute one or more fraudulent transactions involving sellers using the updated personal details. Therefore, the existence of fraudulent personal details submitted to an account issuer is indicative that subsequent transactions attempted with the chargeable account are more likely to be fraudulent transactions. Thus, knowledge of the circumstances under which stored personal details were submitted allows a seller or other interested party to better discern between a legitimate buyer and a fraudster.

In particular embodiments, the reliability indicators of embodiments of the present invention may be used to augment existing techniques for verifying personal

details. Specific examples of these existing techniques are based upon comparing at least one candidate personal detail with at least one stored personal detail.

According to various embodiments, at least one reliability indicator is based on a time at least one stored personal detail was received, an identification procedure performed upon receipt of at least one stored personal detail, and/or the degree of personal exposure of the person who submitted at least one stored personal detail.

In specific embodiments, a more recent submission time increases the estimated likelihood that at least one stored personal detail was submitted fraudulently, and concomitantly increases the estimated likelihood that one or more proposed transactions involving a seller are fraudulent.

In specific embodiments, a lower degree of personal exposure increases the estimated likelihood that at least one stored personal details was submitted fraudulently, and concomitantly increases the estimated likelihood that one or more proposed transactions involving a seller are fraudulent.

In specific embodiments, submission of at least one stored personal detail using the Internet increases the estimated likelihood that the at least one stored personal detail was submitted fraudulently.

In specific embodiments, submission of at least one stored personal detail in person decreases the estimated likelihood that the at least one stored personal detail was submitted fraudulently.

In specific embodiments, the presentation of a verifying item upon submission of at least one stored personal detail decreases the estimated likelihood that at least one stored personal detail was submitted fraudulently, and concomitantly decreases the estimated likelihood that one or more proposed transactions involving a seller are fraudulent. Exemplary verifying items include but are not limited to government issued identification, a hand signature and biometric information.

In particular embodiments, fraud prevention measures based upon the provided at least one reliability indicator are carried out.

Exemplary fraud prevention measures include but are not limited to:
making a phone call to a verified phone number, sending an email to a verified email address, and/or physically sending an item to a verified street address.

In particular embodiments, the methods provided further comprise authorizing or denying a transaction based upon the determined reliability of candidate personal details.

Exemplary personal details include but are not limited to the account owner's name, his street address, his phone number, his email address, his government-issued identifier, a billing address, an additional address, a mother's maiden name, and/or a social security number.

According to some other aspects, the present invention provides a verification system for determining the reliability of a transaction involving an account identifier identifying a chargeable account. This verification system includes a data receiving unit configured to receive data selected from the group consisting of the account identifier and at least one candidate personal detail, a reliability indicator provider for providing at least one reliability indicator indicating the estimated likelihood that at least one stored personal detail associated with the chargeable account was submitted fraudulently; and optionally a data output unit configured to output data.

These and further embodiments will be apparent from the detailed description and examples that follow.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 provides a block diagram of specific embodiments of the present invention involving a buyer, a seller and verification system.

Fig. 2 provides a flow chart of specific embodiments of the present invention.

Fig. 3 provides a flow chart of specific embodiments of the present invention wherein at least one candidate personal detail is compared to at least one stored personal detail.

Fig. 4 provides a diagram of an exemplary system of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

Prior to setting forth the invention, it may be helpful to an understanding thereof to first set forth definitions of certain terms that are used hereinafter.

As used herein the term "personal details" are any extra information associated with a chargeable account. Examples of "personal details" include but are not limited to the account owner's name, his street address, a billing address, an additional

address, his phone number, his email address, his government-issued identifier, an additional address, a mother's maiden name, a social security number, etc.

It is understood that this chargeable account may but does not necessarily belong to a single person, and may be owned by a group of persons, a business, or any other entity.

As used herein, the term "buyer" refers to any person or entity, which wishes to execute a transaction with a "seller" by using a chargeable account. In different contexts, the term "buyer" may refer to the true owner of the chargeable account, to a person authorized by the true owner, or to a fraudster impersonating the true owner.

As used herein, the term "stored personal details" relates to personal details submitted to a party other than the seller. The stored personal details may be submitted by any entity, including the true owner of the account or a fraudster. In particular embodiments, these details are submitted to an organization administering the chargeable account, or to a party storing data related to the chargeable account. In particular embodiments, these stored personal details are stored in computer memory, computer readable media or on human readable media such as ink on paper.

As used herein, the term "candidate personal details" or "presented personal details" both refer to any personal details submitted by a buyer or other interested entity in relation to the account identifier.

As used herein, "reliability indicators" are information indicating an estimated likelihood that at least one stored personal details associated with the chargeable account were submitted fraudulently.

One exemplary reliability indicator is the identification procedure performed when the stored personal details were received. Secure identification procedures increase their reliability, in comparison to less secure procedures. An identification procedure is considered secure if it is more difficult for a fraudster impersonating another person to pass it successfully compared to a person using his real identity. For example, if the information was received in a fax along with a photocopy of the account owner's government-issued ID, the information should be considered more reliable than if the information was faxed with no identifying document.

Another exemplary reliability indicator is the level of exposure taken by the person who supplied the information. In this context, exposure is defined as the

difficulty to apprehend a person if he is determined to be a criminal. Fraudsters usually try to avoid apprehension, and therefore try to minimize exposure as much as possible. Therefore, a transaction in which a person exposes himself is less likely to be fraudulent. For example, if the information was received in the physical presence of the person it can be considered more reliable than if it was received in an anonymous Internet communication.

Another indicator is the time at which the information was received. Information that was received a long time before a buyer contacted a seller to request a transaction may be considered more reliable than information received more recently. Time affects reliability since fraudsters usually use a specific identity for a short time (e.g. they obtain a stolen credit card and quickly perform several charges until it is blocked). Therefore, information submitted a long time in the past is less likely to be part of a scam currently conducted by buyer, than information that was received recently.

Similarly, any other evidence that shows the information was provided without fraudulent intentions may be used.

The present inventors have developed methods for verifying and assessing the reliability of a transaction involving a chargeable account, by using at least one reliability indicator.

Fig. 1 describes the environment related to certain embodiments of the invention. Buyer **100** wishes to obtain a product or service from Seller **102.** Buyer **100** provides Seller **102** with chargeable account identifier and candidate personal details. If Buyer **100** is the account owner or one authorized by the account owner, the transaction is legitimate. If Buyer **100** is not the account owner and is not authorized by him, the transaction is fraudulent.

Examples of chargeable account identifiers include but are not limited to a credit card number, a debit card number, a checking account number, a bank account identifier, a phone number or any identifier that would allow Seller **102** to charge an account. In certain embodiments, Seller **102** obtains an account identifier, candidate personal details or parts thereof from a source other than Buyer **100.** In other embodiments, Seller **102** obtains the account identifier without candidate personal details. In one exemplary embodiment, Buyer **100** contacts Seller **102** by phone or SMS and Seller **102** subsequently obtains Buyer **100**'s phone number (the account

identifier) using the Caller ID service or from information received with the SMS message. In another exemplary embodiment, Buyer **100** provides his name, and Seller **102** retrieves the street address or phone number of Buyer **100** from a white pages directory.

Seller **102** then forwards the account identifier and optionally the candidate personal details to Verification System **104**.Verification System **104** returns at least one reliability indicator, and optionally stored personal details.

Fig. 2 describes exemplary steps taken by Verification System **104**.

First, Verification System **104** receives an account identifier and optionally candidate personal details (step **202**). The Verification System **104** then optionally retrieves personal details (step **204**). In certain embodiments, these stored personal details are retrieved from an account database (step **204**). For example, this database may be the customer database of a credit card issuer (or a replica of it), containing the cards' details, cardholders' personal information and history of interactions between the issuer and the cardholders. In another example, this database is the transaction history of a credit card processing service, containing for each transaction the card's details and the cardholder personal information submitted with it.

In embodiments described in Fig. 2, the Verification System **104** next retrieves reliability indicator(s) (step **208**), and then sends the reliability indicator(s) and optionally the stored personal details (step **210**).

Fig. 3 provides illustration of embodiments wherein candidate personal details are received and wherein the received candidate personal details are compared to stored personal details (step **210**).

In specific embodiments, this comparison between candidate and stored personal details is carried out by seeking a literal match. For example, an email address provided in the candidate personal details may be found to be identical to an email address in the stored personal details. In other embodiments, comparison is done by seeking a partial literal match. For example, candidate personal details may contain a US 5-digit zip code that matches the beginning of a US 9-digit zip code found in the stored personal details. Comparison may also be done by looking for a match with spelling difference (e.g. 'Forty-Second St.' and '42nd street') or a nickname match (e.g. 'Tom' and 'Thomas'). The match between the candidate and stored personal details can also be based on a directory listing. In one exemplary

embodiment, the candidate personal details include a name, the stored personal details include a phone number, and a phone directory listing shows the name and phone number match. The match between the candidate and stored personal details can also be based on a combination of any of the match types above.

The comparison results can be expressed in various ways. One option is to provide a match / no-match flag. If several items are available in the details, a flag may be provided for each item (e.g. "name: no match, street address: match, zip code: match"). Another option is to provide a match score, wherein high scores indicate a strong match and low scores indicate a weak match (e.g. "John Smith" compared to "John Smith" will get a higher score than "J D Smith" compared to "John Smith", which in turn will get a higher score than "David Jones" compared to "John Smith").

In embodiments described in Fig. 3, at least one reliability indicator is subsequently retrieved (step **208**). Although shown this way in Fig. 3, it is not a requirement of the present invention that the candidate personal identifiers be compared with the stored personal identifiers (step **206**) before the at least one reliability indicator are retrieved (step **208**). Thus, in other embodiments, the at least one reliability indicator are retrieved (step **208**) before the actual comparison step **206**.

Reliability indicators may also be derived by data mining a training set including potential reliability indicators with potential predictive power using techniques known from the fields of statistics or machine learning. In particular embodiments, this training set includes data about the potential reliability indicators and data about whether proposed transactions included elements of fraud or not. Exemplary techniques include but are not limited to C45 trees, Hidden Markov Models, Neural Networks, or meta-techniques such as boosting or bagging. In specific embodiments, this statistical model is created in accordance with previously collected "training" data. Appropriate statistical techniques are well known in the art, and are described in a large number of well known sources including, for example, Data Mining: Practical Machine Learning Tools and Techniques with Java Implementations by Ian H. Witten, Eibe Frank; Morgan Kaufmann, October 1999), the entirety of which is herein incorporated by reference.

Verification System 104 may create a new reliability indicator based on analysis of existing reliability indicators. In specific embodiments, this new reliability indicator is created by using a statistical model created in accordance with known statistical

techniques, or known techniques from the field of data modeling. The skilled practitioner is directed to Data Mining: Practical Machine Learning Tools and Techniques with Java Implementations by Ian H. Witten, Eibe Frank; Morgan Kaufmann, October 1999).

In one exemplary embodiment, the exact time at which information was received is replaced with a threshold-based indicator such as 'old' for information received over 1 year ago, 'recent' for information received between 1 month and 1 year ago, and 'very recent' for information received in the last month. In another embodiment, a reliability score between 0 and 100 is generated based on an analytical model that combines several reliability indicators (e.g. identification procedure, exposure level and time). In another embodiment, a flag is generated based on all available reliability indicators, which can be equal to either 'reliable' or 'unreliable'.

In particular embodiments, the at least one reliability indicator is provided implicitly to Seller **102**. In one exemplary embodiment, Verification System **104** is configured to inform Seller **102** that candidate personal details don't match stored personal details if Verification System **104** has determined that stored personal details are not reliable (even if candidate personal details do in fact match stored personal details). In this exemplary embodiment, a response from Verification System **104** informing Seller **102** that candidate personal details match stored personal details, contains an implicit indicator that the personal details are reliable. This exemplary embodiment allows introduction of implicit reliability indicators into computer systems that have not been specifically adapted to handle explicit reliability indicators.

Finally, Verification System **104** sends to Seller **102** the results of the comparison process and the one or more reliability indicators (step **212**). If different matching elements in the stored personal details have different reliability, separate reliability indicators may be reported for each. In one example, both a name and a billing address in the candidate personal details are found to match the stored reliability details, but the name is found to be provided 2 years ago in the presence of the person who opened the account, while the address was changed over the phone 3 days ago. In this case, the response may include a different reliability indicator for each of the name and address.

After receiving the response, Seller **102** will in specific cases perform some action based on the response. For example, if the comparison results indicate that candidate personal details doesn't match the stored personal details, or if the reliability indicator indicates low reliability, Seller **102** may reject Buyer 100's transaction. In another example, if a phone number is reported matching and reliable, Seller **102** may call that number and verify that Buyer **100** answers the phone (e.g. check that the person who answers is aware of the transaction). In another example, if a mailing address is reported matching and reliable, Seller **102** may ship a product requested by Buyer **100** to this address. In another example, if an email address is reported matching and reliable, Seller **102** may send an email to that address and verify that Buyer **100** can access the email (e.g. by requiring Buyer **100** to provide Seller **102** with a secret code sent in the email).

In another preferred embodiment of the present invention, Seller **102** provides to Verification System **104** the account identifier without candidate personal details, and Verification System **104** provides in response stored personal details and the one or more reliability indicators. Seller **102** can then use the information contained in the stored personal details the same way he used the verified elements in candidate personal details in the previous embodiment. In this embodiment there is also no need for Buyer **100** to provide candidate personal details to the Seller **102.**

Fig. 4 describes the components of the system in accordance with a preferred embodiment of the present invention.

A Data Receiving Unit **30** receives an account identifier and optionally candidate personal details from an entity outside of the Verification System **104.** In particular embodiments, this entity is the Seller **102.** The Data Output Unit **32** outputs the at least one reliability indicator, and optionally comparison results and optionally one or more stored personal details. It is noted that data may enter or leave the Verification System **104** through any applicable medium, such as a private data network, the Internet, IVR, modem etc.

In the embodiment shown in Fig. 4, the Reliability Indicator Provider **40** retrieves at least one reliability indicator and optionally stored personal details, by connecting to Account Database **38.** In one particular embodiment, the account database is a relational database such as those available from Microsoft (Redmond, Washington) or Oracle (Redwood Shores, Ca). In one particular embodiment, the

account identifier, the stored personal details and the at least one reliability indicator are associated in the Account Database. Account Database **38** may be physically part of Verification System **104** or an external component accessible over any applicable medium.

Optional Comparison Module **34** compares candidate and stored personal details to determine whether they match, as described above.

The Reliability Indicator Provider **104** is optionally further configured to create at least one reliability indicator based on analysis of retrieved reliability indicators, as described above.

While particular embodiments of the invention have been shown and described, it will be obvious to those skilled in the art that changes and modifications may be made without departing from the invention in its broader aspects, and therefore, the aim in the appended claims is to cover all such changes and modifications as fall within the true spirit and scope of the invention.